UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

CHRISTOPHER GEORGE PABLE, *Plaintiff*, v. CHICAGO TRANSIT AUTHORITY and CLEVER DEVICES LTD., *Defendants*.	Case No. 19-cv-7868 Judge Elaine E. Bucklo Magistrate Judge Heather K. McShain
CHICAGO TRANSIT AUTHORITY, *Counter-Plaintiff*, v. CHRISTOPHER GEORGE PABLE, *Counter-Defendant*.	

CHICAGO TRANSIT AUTHORITY'S
REPLY IN SUPPORT OF ITS MOTION TO COMPEL PLAINTIFF TO PRODUCE HIS CELL PHONE FOR INSPECTION AND IMAGING AND RESPOND TO THE CTA'S REQUEST FOR PRODUCTION

In his Response in Opposition to the CTA's Motion to Compel (the "Response"), Plaintiff forgoes arguments supported by legal authority and instead presents factual omissions and oversimplifications to suggest that his cell phone should not be reimaged, and that he need not produce archived copies of his personal website. Plaintiff maintains, without *any* evidentiary support, that his phone is now devoid of data and information because the CTA "wiped" it upon his departure in October 2018. Plaintiff's version of events strains credulity and is not an acceptable rationale to support Plaintiff's argument that he can withhold relevant information from the CTA when the phone itself is implicated in the litigation. And, Plaintiff's proposed solution—to require the CTA to explore these issues in depositions before ordering re-imaging the phone (Dkt. 47 at 10)—will likely result in further motion practice and a second round of

depositions for Plaintiff and potentially others so that the CTA can inquire into new evidence obtained from the device once this dispute is resolved.

The CTA has demonstrated that Plaintiff's cell phone is material to the claims and defenses at issue in the litigation, and that the image file of the phone produced to the CTA is incomplete or otherwise compromised based upon both its careful review of other discovery and its third-party vendor's own in-depth analysis of the produced image file. For the reasons set forth herein and in the CTA's Motion, this Court should compel the production of Plaintiff's cell phone for re-imaging and archived copies of Plaintiff's personal website.

I. The CTA is Entitled to the Production and Re-Imaging of Plaintiff's Cell Phone.

As detailed in its Motion, the CTA seeks the production of Plaintiff's personal cell phone for inspection and re-imaging in a manner consistent with industry standards for three reasons: (i) Plaintiff failed to produce relevant communications that the CTA knows exists and have not yet been produced by Plaintiff, but may continue to exist on the phone; (ii) the phone itself is directly implicated in the CTA's affirmative defenses to Plaintiff's claim against the CTA, in the CTA's CFAA counterclaim against Plaintiff, and in Plaintiff's defenses thereto; and (iii) the image file produced to the CTA is completely devoid of any data. Specifically, the CTA alleges in its counterclaim that Plaintiff encrypted his CTA computer at multiple points of access without the CTA's authorization or knowledge, including through the use of encryption applications installed on his phone. (Dkt. 45 at 3-4.) Plaintiff's proffered defense to the CTA's counterclaim directly relies on the *same* phone, where Plaintiff contends "[a]ny inability or other difficulties associated with accessing data on Pable's computer is the direct result of the CTA's conduct . . . the CTA's unilateral decision, with no notice or warning to Pable, to disable access to certain data stored on Pable's phone, eliminated the ability to access the encrypted data on the

Computer." (Dkt. 34.) Plaintiff's attempts to preclude the CTA from discovering information relevant to its counterclaim and affirmative defenses give rise to spoliation concerns.

A. As Plaintiff repeatedly acknowledges in his Response, his cell phone is directly implicated in the litigation.

Plaintiff makes clear in his Response that his cell phone is central to the CTA's counterclaim, reinforcing the CTA's need for further discovery into the device. Plaintiff repeatedly claims that in or around October 2018, "the CTA disabled the profile on [Plaintiff's] phone under which substantially all of his work-related communications and applications had been installed, effectively preventing him (or anyone else) from accessing this data." (Dkt. 47 at 3; *see also id.* at 6, 9.) But to date, Plaintiff has offered no evidence in support of these dubious claims, which the CTA denies. (Dkt. 45 at n.2.) Similarly, the CTA's review of the produced phone image did not reveal any evidence that the CTA "wiped" seemingly all information from the device. An appropriate image of the phone may reveal more evidence relevant to this purported "wipe," including how it was done and by whom (if at all).[1]

Plaintiff attempts to distinguish this case from the Court's decision in *Belcastro v. United Airlines* to argue that a forensic imaging of his cell phone is not necessary because his cell phone is not central to the conduct at issue, and because the *Belcastro* plaintiff "had not retained a professional to search for and extract data from his phone." (Dkt. 47 at 7) (citing 2019 WL 7049914 (N.D. Ill. Dec. 23, 2019)). Plaintiff's reliance on *Belcastro* is inapposite, as that case supports the CTA's request to re-image Plaintiff's phone where Plaintiff (and/or his vendor) have failed or otherwise refused to produce a complete image containing all data relevant to the

[1] At most, the CTA would have disabled Plaintiff's access to the CTA network and/or CTA email on his phone, as it would for any employee put on leave or whose employment is terminated. The CTA would have no means of knowingly disabling or wiping an employee's personal phone completely. If the CTA somehow unknowingly caused a wipe, it should be permitted on that basis to investigate these actions on an image of the phone.

litigation. As detailed in the Motion, Plaintiff's own "piecemeal production of responsive documents" in this case demonstrates that Plaintiff (or his third-party vendor) "lacks the expertise necessary to search and retrieve all relevant data" from the phone such that re-imaging is necessary. *Belcastro*, 2019 WL 7049914, at *3. The CTA's third-party vendor's review of the image file supports the inference that the phone was not imaged by a vendor with the expertise necessary to fully capture relevant data on the phone. (*See* Dkt. 45-1 at Ex. H, ¶ 13 noting that, *inter alia*, the logical phone image file produced by Plaintiff did not collect the database that would contain Signal messages.) The fact that Plaintiff presents himself to the public as a hacking expert and sophisticated computer technician furthers the CTA's growing concerns that Plaintiff is deliberately withholding relevant information or has already engaged in the spoliation of evidence.

B. The CTA has unequivocally demonstrated that the phone image produced by Plaintiff in discovery is compromised or incomplete; those deficiencies will (or should be) cured by re-imaging his cell phone.

As the CTA's Motion demonstrates in detail, Plaintiff has shirked his discovery obligations in this case for nearly a year, and his attempt to persuade this Court to the contrary is unavailing. While it is true that Plaintiff has produced some communications relevant to this matter, including in supplemental production sets (Dkt. 45 at 5-6), Plaintiff's production is still incomplete. For instance, Plaintiff contends he produced "screen shots[2] of his cell phone" supposedly reflecting the "'real world' look and feel of the messages [exchanged in Google Hangouts and via the Signal encrypted messaging application] accessible from his cell phone at

[2] Plaintiff incorrectly characterizes the *photographs* he produced of certain messages exchanged via Google Hangouts or Signal as "screen shots." (Dkt. 47 at 5.) As the CTA's Motion demonstrates, (Dkt. 45 at 7), the Plaintiff actually produced scanned PDFs of photographs taken by an individual holding what Plaintiff claims is his phone, depicting various portions of messages on the phone screen.

the time of its forensic information." (Dkt. 45 at 5.) But this unsophisticated and inadequate production methodology does retain the same functionality as the native files, and not comport with the CTA's specified production protocol. *See, e.g., EEOC v. SVT, LLC*, 2014 WL 1411775, No. 2:13-CV-245-RLM-PRC, *6 (N.D. Ind. April 4, 2014) (a court will compel production of native files where image files will not keep the same functionality of the native file); *see also Autotech Techs. Ltd. Partn. v. Automationdirect.com, Inc.*, 248 F.R.D. 556 (N.D. Ill. 2008) (declining to compel the production of certain metadata where defendant did not request it as a part of its discovery requests). Moreover, the photographs are devoid of relevant metadata affiliated with the messages themselves, which is necessary for authenticating, *inter alia*, the times and dates of the messages sent, the identity of the corresponding parties, and whether the contents of the messages themselves have been altered or deleted. The CTA has repeatedly sought a complete forensic image of Plaintiff's phone since March 2020 and is entitled to inspect the associated metadata that should accompany such an image file if it is prepared in accordance with industry standards.

Plaintiff's supplemental production and discovery obtained by the CTA from third parties demonstrate that information relevant to the CTA's claims and defenses is likely being withheld or, worse still, has already been destroyed. For instance, Plaintiff contends that his expert was able to access some of Plaintiff's Google Hangouts and Signal communications on the phone that were ultimately produced to the CTA in photographs. (Dkt. 47 at 10.) While the phone image produced to the CTA was created on June 11, 2020 (Dkt. 45-1 at Ex. H, ¶ 11), the photographs purportedly depicting messages exchanged on the phone were taken *the following day* – on June 12, 2020. (Dkt. 45-1 at Ex. I.) Even though a portion of Plaintiff's messages was clearly available and accessible on the phone *after* the forensic phone image was created such that someone could take a photograph of them as they appeared on the phone screen, the CTA's

third-party vendor's review of the phone image revealed *no trace* of the Signal and Google Hangouts messages depicted in the photographs. (Dkt. 45-1 at Ex. H, ¶¶ 12-14.) As a result, the CTA's third-party vendor concluded that "[i]t is evident that communication data does exist on the device that was not contained within the forensic image." (Dkt. 45-1 at Ex. H, ¶ 14.)

Moreover, Plaintiff has yet to produce *a single text message* exchanged between Plaintiff and his supervisor, Michael Haynes ("Haynes") – even though Haynes separately produced dozens of relevant text messages exchanged by and between Plaintiff *after* their November, 2018 departure from the CTA in response to the CTA's subpoena. Even if the CTA "wiped" Plaintiff's phone in October, 2018 at he contends (which it did not), then his subsequent relevant text messages (exchanged with, at minimum, Haynes) should have been preserved and produced by Plaintiff, who at all times had an independent duty to preserve and produce relevant evidence. *Webb v. CBS Broad., Inc.*, No. 08 C 6241, 2010 WL 2104179, at *5 (N.D. Ill. May 25, 2010) (rejecting plaintiff's position that the defendant should simply issue third parties subpoenas for discovery plaintiff should have; a party "cannot simply piggyback on [another party's] discovery efforts"). Plaintiff offers no explanation or evidence in support of its apparent contention that the CTA possesses the ability to continuously wipe all data from a former employee's personal cell phone on a rolling basis for several years.

Other significant facts presented by the CTA in its Motion prove that the phone image is incomplete and are unrefuted by Plaintiff, including:

- The data from the image file only contained about 0.2 GB of data, or about 0.625% of the total device[3]; (Dkt. 45-1 at Ex. H, ¶ 9);

[3] The fact that the produced image of the phone contains effectively no data also begs the question: why would Plaintiff object to an imaging of that same phone?

- The image file contained no MMS messages, instant messages, or internet history, and only contained five irrelevant SMS messages from May 2020; (*id*. ¶ 10);
- Besides the call history, the image file contains *no data* that predates June 5, 2020; (*id*. ¶ 13); and
- The software used to create the image file shows that the phone's affiliated SD card, which stores recordings and messages, was not present in the phone when the image was created (meaning that an entire storage system affiliated with the phone was inexplicably excluded from the image process) (*id*. ¶ 9).

Moreover, certain emails produced by Plaintiff indicate he was actively using the same cell phone that is the subject of the Motion as recently as June 2020. In his June 17, 2020 email to an individual identified only as "dead fish," Plaintiff explains in relevant part that the CTA "now wanted copies of the phone" in this case, which he "still used . . . until a few days ago," and on which he stored "encryption keys to assets [the CTA] own[s]." (*See* relevant portions of Plaintiff's June 2020 email correspondence with "dead fish," P001601-03, attached hereto as Exhibit A.) Even if the CTA "wiped" Plaintiff's phone in October 2018 (which it did not), then the phone image should still contain other data and information accrued during regular use during the period of Plaintiff's departure and through the time of imaging in June 2020. Yet, it does not. Plaintiff further admits to "dead fish" that he was "moving all [his] data" in the process of turning over his phone for imaging. (*Id*.) Plaintiff's emails to "dead fish" suggest Plaintiff transferred or deleted relevant data from the phone he used in 2018 immediately prior to imaging it in this litigation, which may now explain why the phone image produced to the CTA is completely devoid of data.

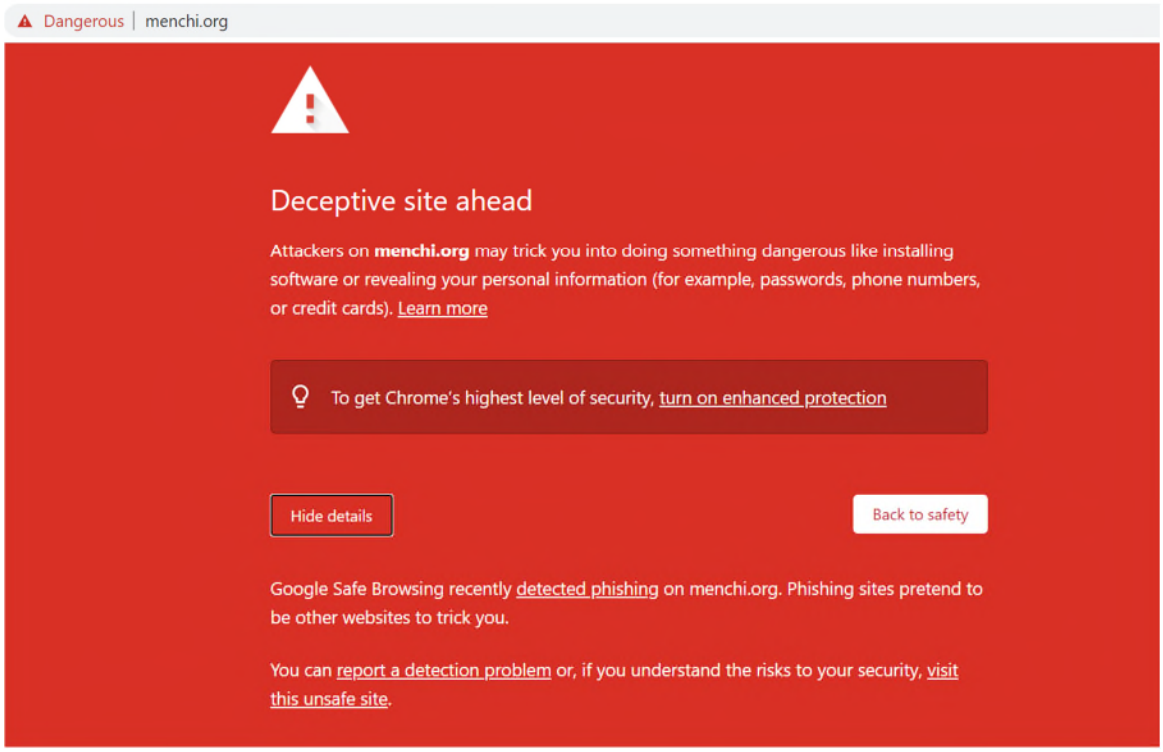
II. The CTA is Likewise Entitled to Complete and Accurate Copies of Plaintiff's Archived Personal Website.

In his Response, Plaintiff indicates that that there is "not much to [the] issue" relating to the CTA's request for copies of Plaintiff's archived personal website "on which he mostly posts pictures of his dog." (Dkt. 47 at 10.) Plaintiff's characterization of his website is, at best, misleading. While www.menchi.org appears to be named after Plaintiff's dog and does contain pictures of dogs, Plaintiff's personal website effectively served as an interactive resume, wherein he described various personal and professional technical projects in great detail. On or about October 15, 2020, the CTA captured screenshots of detailed and proprietary information about certain proprietary CTA technology projects on the website, which give rise to security concerns and may lead to other relevant evidence in this case. Thereafter, Plaintiff deleted that information[4], seemingly without preserving it, and has since refused to reproduce it. The CTA's October 15, 2020 screenshots of www.menchi.org capture Plaintiff's website as it existed for only a moment in time. But the CTA is entitled to Plaintiff's full archived website in order to

[4] In his Response, Plaintiff represents that he linked certain code to www.menchi.org "for the benefit of the CTA," and that "[c]ounsel for the CTA requested [Plaintiff] to take down the code, and he did." (Dkt.47.) Plaintiff's representations erroneously conflate two separate issues pertaining to the CTA's code that are detailed in the CTA's November 24, 2020 Rule 37.2 letter to Plaintiff. (Dkt. 45-1 at Ex. J.) Specifically, in or around October 2020, the CTA discovered that Plaintiff made publicly accessible online code that was developed for the CTA's benefit in furtherance of its Transit Signal Priority project, which assists the CTA buses in extending traffic signal lights. The CTA did not authorize this code to be open source code available on any publicly accessible platform and accordingly demanded that Plaintiff take down this code. Plaintiff did so on December 4, 2020. In or around October 2020, the CTA also discovered www.menchi.org, and captured screenshots of its contents on October 15, 2020. At that time, and as captured in the screenshots, Plaintiff's website contained additional detailed and proprietary information about certain CTA projects. Thereafter, Plaintiff deleted the CTA project information from his website on or about October 28, 2020 – the same date that CTA served Plaintiff with Supplemental Document Requests specifically requesting copies of the archived website.

review any other relevant CTA materials that he may have posted during the course of his employment with CTA or thereafter.

Notably, since the CTA filed its Motion, www.menchi.org has been designated as a "dangerous" and "deceptive site" by Google Safe Browsing, warranting the below security warning to all visitors seeking to access the website as recently as February 19, 2021:



The CTA is currently unaware of whether these new security concerns surrounding www.menchi.org will impact the preservation and availability of the website's contents going forward, and whether the CTA's proprietary information that was once shared by Plaintiff on the website is compromised as a result. Given the apparently compromised status of the www.menchi.org site, it is important to obtain complete and accurate archived copies of all personal websites owned or operated by Plaintiff, including www.menchi.org, in order to prevent the destruction or alteration of relevant evidence. If Plaintiff truly maintains no such archive of his personal website exists, as he suggests in his Response (Dkt. 45 at 11), even though he

unquestionably deleted relevant information from his website *during the pendency of this litigation*, then the CTA reiterates its request that the Court find Plaintiff has acted in bad faith and give an adverse inference instruction pursuant to Fed. R. Civ. P. 37(e)(2)(B).

WHEREFORE, the CTA respectfully requests that the Court grant this motion and enter an order compelling Plaintiff to: (i) produce to the CTA his cell phone, along with any and all affiliated SD card(s) and/or storage devices to the CTA for inspection and re-imaging; and (ii) respond to the CTA's Requests for Production relating to his personal website, including by producing complete and accurate archived copies of any personal websites owned or operated by Plaintiff, including but not limited to www.menchi.org, as they appeared from May 1, 2018 through the present. The CTA further respectfully requests this Court order Plaintiff to pay the CTA's expenses incurred in making this motion, including attorney's fees, as provided under Fed. R. Civ. P. 37(a)(5), as well as any other Rule 37 sanction this Court deems appropriate in light of Plaintiff's failure to comply with his discovery obligations, and grant all other relief it deems appropriate.

Dated: February 19, 2021

Respectfully submitted,

CHICAGO TRANSIT AUTHORITY

By: *s/ Elizabeth E. Babbitt*
One of Its Attorneys

John F. Kennedy
jkennedy@taftlaw.com
Elizabeth E. Babbitt
ebabbitt@taftlaw.com
Allison E. Czerniak
aczerniak@taftlaw.com
Nicollette L. Khuans
nkhuans@taftlaw.com
TAFT STETTINIUS & HOLLISTER LLP
111 East Wacker, Suite 2800
Chicago, Illinois 60601
(312) 527-4000